

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#)

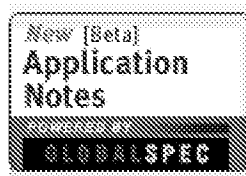
Welcome United States Patent and Trademark Office

[Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Results for "((bilinear party association secret shared key)<in>metadata)"

Your search matched 0 of 1931036 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

[» Search Options](#)[View Session History](#)[New Search](#)[» Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

☐ Check to search only within this results setDisplay Format: ☒ Citation ☐ Citation & Abstract[IEEE/IET](#)[Books](#)[Educational Courses](#)[A](#)

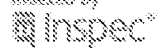
IEEE/IET journals, transactions, letters, magazines, conference proceedings, and

[Select All](#) [Deselect All](#)

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistance.

Indexed by

[Help](#) [Contact Us](#)

© Copyright 2008



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

-

Ad
Sc
Sc

Scholar [All articles](#) - [Recent articles](#) Results 1 - 10 of about 47 for bilinear secret shared private k

Lattice Reduction in Cryptology: An Update

PQ Nguyen, J Stern - LECTURE NOTES IN COMPUTER SCIENCE, 2000 - Springer
... the one hand, there are very few public-key cryptosystems based ... settings such as low public or private exponent. ... 1), and therefore all the bases share the same ...
[Cited by 81](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 8 versions](#)

[PDF] ► Multimedia authenticity with ICA watermarks

S Noel, H Szu - PROC SPIE INT SOC OPT ENG, 2000 - ise.gmu.edu
... stretching, shearing, rotation), followed by resampling using bilinear interpolation. ... idea is that the sender and receiver share a secret key for generating ...
[Cited by 11](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 9 versions](#)

The Two Faces of Lattices in Cryptology

PQ Nguyen, J Stern - LECTURE NOTES IN COMPUTER SCIENCE, 2001 - Springer
... one hand, there are very few public-key cryptosystems based ... settings such as low public or private exponent, but ... 1), and therefore all the bases share the same ...
[Cited by 94](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 13 versions](#)

Multimedia watermarking techniques - ► [frank-hartung.com](#) [PDF]

F Hartung, M Kutter - Proceedings of the IEEE, 1999 - ieeeexplore.ieee.org
... While such techniques often share similar principles and basic ... a public key and the other with a secret key. ... several public keys with a private key and embeds ...
[Cited by 763](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 14 versions](#)

[PDF] ► of Deliverable New Trends in Cryptology

P Nguyen - resonance, 2001 - stork.eu.org
... network-wide level, all pebblenets share a traffic ... signer might intentionally disclose his private signature key ... a secure distribution of secret data necessary ...
[Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 6 versions](#)

[CITATION] CD-ROM Project Macedonian Antiquities

D DISOSKI, K TRAJKOVSKI, V PETROVSKA, S MITEVSKI, P ... - Futurefusion: Application Realities for the Virtual Age: ..., 1998 - IOS Press
[Related articles](#) - [Web Search](#)

[BOOK] Climbing the Mountain: The Scientific Biography of Julian Schwinger

J Mehra, KA Milton - 2000 - books.google.com
... Due to this close association, he gained an intimate ... this extremely complex and extraordinarily private man ... 3 As they grew up, Harold and Julian shared a large ...
[Cited by 17](#) - [Related articles](#) - [Web Search](#) - [Library Search](#) - [All 6 versions](#)

HYPOTHESES The Making of Bamana Sculpture: Creativity and Gender. By SARAH C. BRETT-SMITH. Cambridge ...

TAL TAMARI - The Journal of African History, 1999 - Cambridge Univ Press
... meta-systems in which shared codes of ... his structural approach and his association of absolutism ... requisite material conditions (including private land ownership ...
[Web Search](#)

Historical Dictionary of Tunisia. By KENNETH J. PERKINS. London: The Scarecrow Press, Inc. 1997. Pp. ...

M TESSLER - The Journal of African History, 1999 - Cambridge Univ Press

... meta-systems in which shared codes of ... his structural approach and his association of absolutism ... requisite material conditions (including private land ownership ...

[Web Search](#)

HISTORICIZING CULTURAL EXPRESSION Inventing Masks: Agency and History in the Art of the Central ...

W MACGAFFEY - The Journal of African History, 1999 - Cambridge Univ Press

... meta-systems in which shared codes of ... his structural approach and his association of absolutism ... requisite material conditions (including private land ownership ...

[Web Search](#)

Key authors: [P Nguyen](#) - [J Stern](#) - [F Hartung](#) - [M Kutter](#) - [J Mehra](#)

Goooooogle ►

Result Page: 1 2 3 4 5 [Next](#)

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

bilinear secret shared private key trusted component 1996

- 2002

Ad
Sc
Sc

Scholar All articles - [Recent articles](#) Results 1 - 10 of about 20 for bilinear secret shared private key

[An Identity-Based Signature from Gap Diffie-Hellman Groups](#) - [grsu.by](#) [PDF]

JC Cha, JH Cheon - LECTURE NOTES IN COMPUTER SCIENCE, 2002 - Springer
... Given a secret key D ID and a message m , pick a ... 1 can be obtained using the non-degenerated bilinear map, since ... described in [BF01] can be shared with ...
Cited by 361 - [Related articles](#) - [Web Search](#) - [BL Direct](#) - All 12 versions

[Identity Based Authenticated Group Key Agreement Protocol](#)

KC Reddy, D Nalla - LECTURE NOTES IN COMPUTER SCIENCE, 2002 - Springer
... This sponsor is responsible for updating its secret key ... share, computing affected [key, Bkey] pairs and broadcasting all Bkeys of the new tree to ... 1. Bilinear ...
Cited by 20 - [Related articles](#) - [Web Search](#) - [BL Direct](#) - All 4 versions

[Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group ...](#) - [ucsd.edu](#) [PDF]

A Boldyreva - LECTURE NOTES IN COMPUTER SCIENCE, 2002 - Springer
... a special structure provided by bilinear maps. ... outputs a public key y . The private output ... correctly by manipulating the distribution of the shared secret key. ...
Cited by 190 - [Related articles](#) - [Web Search](#) - [BL Direct](#) - All 13 versions

[PDF] [Authenticated ID-based key exchange and remote log-in with simple token and PIN number](#)

M Scott - IACR eprint, 2002 - [eprint.iacr.org](#)
... different low entropy secret must be shared between every ... before she partitions her individual secret up between ... an instance of the co-bilinear Diffie-Hellman ...
Cited by 14 - [Related articles](#) - [View as HTML](#) - [Web Search](#) - All 6 versions

[Identity-Based Encryption from the Weil Pairing](#) - [mac.com](#) [PDF]

D Boneh, M Franklin - LECTURE NOTES IN COMPUTER SCIENCE, 2001 - Springer
... as ID-OWE except that there are no private key extraction queries ... key (rather than a public key of her ... satisfies the following properties: 1. Bilinear: For all ...
Cited by 2053 - [Related articles](#) - [Web Search](#) - [BL Direct](#) - All 29 versions

[PDF] [Signature-Masked Authentication Using the Bilinear Pairings](#)

F Zhang, K Kim - Cryptology and Information Security Laboratory (CAIS), ..., 2002 - [uow.edu.au](#)
... Key generation: Secret key: a random number s chosen from ... public key infrastructure from the bilinear pairing [2 ... Then the user cannot share the credential with ...
Cited by 1 - [Related articles](#) - [View as HTML](#) - [Web Search](#) - All 4 versions

[Exponent group signature schemes and efficient identity based signature schemes based on pairings. ...](#) - [kfupm.edu.sa](#) [PDF]

F Hess - 2002 - [eprints.kfupm.edu.sa](#)
... Setup : The signer creates a private-public key pair ... 1. Bilinear: $e(x_1 + x_2, y) = e(x_1, y) e(x_2, y)$... a random element $P \in G$ and a secret integer t ...
[View as HTML](#) - [Web Search](#)

[Cryptography from Pairings: A Snapshot of Current Research](#) - [ksu.edu.sa](#) [PDF]

KG Paterson - Information Security Technical Report, 2002 - Elsevier

... last computational problem is called the Bi-linear Diffie-Hellman ... If the TA's master secret s is disclosed ... two different TAs, but ones which share the same ...

[Cited by 35](#) - [Related articles](#) - [Web Search](#) - [All 4 versions](#)

[A Shape-Preserving Data Embedding Algorithm for NURBS Curves and Surfaces -](#)

► [yamanashi.ac.jp](#) (PDF)

R Ohbuchi, H Masuda, M Aono - Proceedings of Computer Graphics International, 1999 - doi.ieeecomputersociety.org

... Both public- key cryptography and shared-key (or private ... Flow of data in our private data embedding ... rational-linear (alias linear fractional, bilinear, or Mobius ...

[Cited by 83](#) - [Related articles](#) - [Web Search](#) - [All 10 versions](#)

[PDF] ► [Unified approach of asymmetric watermarking schemes](#)

T Furon, I Venturini, P Duhamel - Security and Watermarking of Multimedia Contents III, 2001 - hal.ccsd.cnrs.fr

... relying on completely different concepts, they share the same ... could detect watermarks, hence the term private detection ... The detection may also need a secret key. ...

[Cited by 29](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 11 versions](#)

Key authors: [J Cha](#) - [D Boneh](#) - [J Cheon](#) - [M Franklin](#) - [A Boldyreva](#)

Google ►

Result Page: 1 2 [Next](#)

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2008 Google